

The Economics of Security

George Danezis and Ross Anderson

University of Cambridge, Computer Laboratory

June 17, 2004

Economics of Information Security

- ▶ Over the last four years, we have started to apply economic analysis to information security
- ▶ Economic analysis often explains security failure better than technical analysis!
- ▶ Information security mechanisms are used increasingly to support business models rather than to manage risk
- ▶ Economic analysis is also vital for the public policy aspects of security

Traditional View of Infosec

- ▶ People used to think that the Internet was insecure because of lack of features: crypto, authentication, filtering
- ▶ So engineers worked on providing better, cheaper security features: AES, PKI, firewalls, . . .
- ▶ About 1999, we started to realize that this is not enough

New View of Infosec

- ▶ Systems are often insecure because the people who could fix them have no incentive to
- ▶ Bank customers suffer when bank systems allow fraud; patients suffer when hospital systems break privacy; Amazon's website suffers when infected PCs attack it
- ▶ Security is often what economists call an 'externality': like environmental pollution
- ▶ Provides an excuse for government intervention

New Uses of Infosec

- ▶ Xerox started using authentication in ink cartridges to tie them to the printer
- ▶ Followed by HP, Lexmark . . . and Lexmark's case against SCC, and EU Parliament Directives
- ▶ Motorola started authenticating mobile phone batteries to the phone
- ▶ BMW now has a car prototype that authenticates its major components

IT Economics and Security

- ▶ High fixed/low marginal costs, network effects and switching costs all tend to lead to dominant-firm markets with big first-mover advantage
- ▶ So time-to-market is critical
- ▶ Microsoft philosophy of 'we'll ship it Tuesday and get it right by version 3' is not perverse behaviour by Bill Gates but driven by economics
- ▶ Whichever company had won in the PC OS business would have done the same

IT Economics and Security (2)

- ▶ When building a network monopoly, it is also critical to appeal to the vendors of complementary products
- ▶ E.g., application software developers in the case of PC versus Apple, or now of Symbian versus CE
- ▶ Lack of security in earlier versions of Windows makes it easier to develop applications
- ▶ Similarly, motive for choice of security technologies that dump the support costs on the user (e.g. SSL, PKI, ...)

Where are the good security products?

- ▶ Akerlof's Nobel-prizewinning paper, 'Market for Lemon' provides key insight - asymmetric information.
- ▶ Suppose a town has 100 used cars for sale: 50 good ones worth \$2000 and 50 lemons worth \$1000.
- ▶ What is the equilibrium price of used cars in this town?
- ▶ If \$1500, no good cars will be offered for sale ...
- ▶ Usual fix: brands (eg. 'Volvo certified used cars')

Security and Liability

- ▶ Why did digital signatures not take off (e.g. SET protocol)?
- ▶ Industry thought: legal uncertainty. So EU passed electronic signature law
- ▶ Recent research: customers and merchants resist transfer of liability by bankers for disputed transactions
- ▶ Best to stick with credit cards, as any fraud is the bank's problem
- ▶ Similar resistance to phone-based payment – people prefer prepayment plans because of uncertainty

How are Incentives Skewed?

- ▶ If you are DirNSA and have a nice new hack on NT, do you tell Bill?
- ▶ Tell: protect 300m Americans
- ▶ Don't tell: be able to hack 400m Europeans, 1000m Chinese, . . .
- ▶ If the Chinese hack US systems, they keep quiet. If you hack their systems, you can brag about it to the President and get more budget
- ▶ More research: patching, bug finding, . . .

Why Bill wasn't interested in security

- ▶ While Microsoft was growing, the two critical factors were speed, and appeal to application developers
- ▶ Security markets were over-hyped and driven by artificial factors
- ▶ Issues like privacy and liability were more complex than they seemed
- ▶ The public couldn't tell good security from bad anyway

Why is Bill changing his mind?

- ▶ 'Trusted Computing' initiative ranges from TCG and NGSCB to the IRM mechanisms in Office 2003
- ▶ IRM – Information Rights Management – changes ownership of a file from the machine owner to the file creator
- ▶ Files are encrypted and associated with rights management information
- ▶ The file creator can specify that a file can only be read by Mr. X, and only till date Y
- ▶ What will be the effect on the typical business that uses PCs?

Why is Bill changing his mind? (2)

- ▶ At present, a company with 100 PCs pays maybe \$500 per seat for Office
- ▶ Remember information economics: value of software company = total switching costs
- ▶ So: cost of retraining everyone to use Linux, converting files etc is maybe \$50,000
- ▶ But once many of the documents can't be converted without the creators' permission, the switching cost is much higher
- ▶ Lock-in is the key!

Open or Closed?

- ▶ Free/open source view - easier for defenders to find and fix bugs ('to many eyes, all bugs are shallow')
- ▶ NSA view - easier for attackers to find and exploit bugs
- ▶ Under standard reliability growth model assumptions, openness helps attackers and defenders equally
- ▶ Whether open or closed is better will depend on how your system departs from the ideal

Conclusions

- ▶ Economic analysis of computer security provides good insights (as technical analysis).
- ▶ Security mechanisms fail because of tussle in the real world.
- ▶ Security mechanisms are used as weapons in the tussle and not just for defence!
- ▶ Ultimately it's all about power and control

More ...

- ▶ Economics and Security Resource Page
www.cl.cam.ac.uk/~rja14/econsec.html (or follow link from my home page)
- ▶ Economics of Privacy Page
www.heinz.cmu.edu/~acquisti/economics-privacy.htm